



CALIFORNIA STATE THREAT ASSESSMENT CENTER

24-HOUR REPORT

23 MARCH 2017

(U) NATIONAL

(U) Georgia – Russian Man Pleads Guilty to Over \$500 Million Malware Scam

(U) Atlanta – A Russian man faces up to 10 years in prison for spreading a computer virus that cost victims more than \$500 million. Mark Vartanyan, 29, developed and distributed the Citadel Trojan, which lets criminals steal bank account details and hold files to ransom. The virus had infected about 11 million computers worldwide, according to US prosecutors. The Citadel Trojan was marketed on invitation-only, Russian language internet forums used by cybercriminals. Its users targeted the computer networks of major financial and government institutions around the world. Vartanyan pleaded guilty to one count of computer fraud in a court in Atlanta.

SOURCE: 23 March 2017, [BBC](#)

(U) Wisconsin – Police Officer, Three Others Killed in Wisconsin Town

(U) Weston – A police officer and three other people were shot and killed when a domestic dispute at a bank escalated into shootings at three locations in northern Wisconsin, according to investigators. The shootings occurred Wednesday afternoon at a bank, a law firm and an apartment complex, where officers, including a SWAT team, had a standoff with the suspect for several hours before a shootout. It is currently unclear where the police officer was shot and killed. Police did not disclose the identities of the suspect and the four people who were killed.

SOURCE: 23 March 2017, [AP](#), [Reuters](#)

(U) INTERNATIONAL

(U) Belgium – Man Held for 'Driving at Crowd' on Main Shopping Street

(U) Antwerp – On 23 March, a French national of North African origin was arrested in the Belgian city of Antwerp on suspicion of driving at a crowd, officials say. A car was driven "at high speed" on De Meir, the northern city's main shopping street, before it was intercepted. There were no reports of any injuries. Knives, a non-lethal gun and some unidentifiable liquid were found in the car, prosecutors say. Belgian PM Charles Michel praised the authorities for an "outstanding job". The attack comes a day after a car was driven at high speed along London's Westminster Bridge, hitting many people, before the driver got out and entered the grounds of Parliament. It was also the day Belgium marked the first anniversary of the twin bomb attacks in Brussels that killed 32 people.

SOURCE: 23 March 2017, [BBC](#)

(U) Israel – Israel Police Arrest Suspect in Threats on US Jewish Centers

(U) Jerusalem – Israel police on Thursday arrested a 19-year-old Israeli Jewish man as the primary suspect in a string of bomb threats targeting Jewish community centers and other institutions in the United States and United Kingdom. Scotland Yard and the FBI are investigating more than a hundred bomb threats made to Jewish groups since 7 January. The suspect is described as a hacker, but his motives were still unclear, according to authorities. He has been identified as an American-Israeli dual citizen, according to Israeli media.

SOURCE: 23 March 2017, [AP](#)

(U) Kenya – Kenya Revenue Authority Lost \$39 Million to Hacker

(U) Nairobi – An IT expert has been charged with hacking into Kenya's Revenue Authority and stealing \$39 million. Alex Mutungi Mutuku, 28, is accused of electronic fraud. The prosecution says he is part of an international network stealing money from several state bodies. The government believes there is a ring involving expatriates from the United States and other countries, along with police officers and civil servants. Mutuku is being held while anti-cybercrime officers dig deeper into what they believe is an elaborate fraud scheme with international connections. The cybercrime unit says Kenya lost \$165 through hacking in 2016.

SOURCE: 22 March 2017, [BBC](#)

(U) North Korea – North Korea Said to Be Target of Inquiry Over \$81 Million Cyberheist

(U) Pyongyang – Federal prosecutors are investigating North Korea's possible role in the theft of \$81 million from the central bank of Bangladesh in what officials fear could be a new front on cyberwarfare. The US attorney's office in Los Angeles has been examining the extent to which the North Korea government aided and abetted the heist in February 2016. In the theft, the attackers, using a global payment messaging system known as Swift, were able to persuade the Federal Reserve Bank of New York to move money from the Bangladesh bank to accounts in the Philippines. The Swift system is used by 11,000 banks and companies to transfer money from one country to another.

SOURCE: 22 March 2017, [New York Times](#)

(U) United Kingdom – Eight Arrests as Police Probe Attacker's Links

(U) London – Police investigating what is being considered a terrorist attack in London have arrested eight people in raids around Britain. A tweet from an ISIS-affiliated news agency Amaq said the attacker was a soldier of ISIS inspired by its message. The group did not identify the person behind the attack. The perpetrator was British born and once linked to violent extremism, according to Prime Minister Theresa May. The attacker had been investigated by security services but was regarded as a peripheral figure. The lone attacker plowed a car into crowds of people before stabbing a police officer outside the UK Parliament. Four people were killed and 40 people were injured.

SOURCE: 23 March 2017, [CNN](#), [BBC](#)

(U) PREPARED BY THE CALIFORNIA STATE THREAT ASSESSMENT CENTER.

(U) FOR QUESTIONS OR CONCERNS, PLEASE EMAIL STAC@CALOES.CA.GOV, OR CALL 916-874-1100.

Warning: This document is the exclusive property of the State Threat Assessment Center (STAC) and is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the California Public Records Act (Govt. Code Sec. 6250-6270). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with STAC policy relating to U//FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized STAC official. No portion of this report should be furnished to the media, either in written or verbal form.

This document contains excerpts of suspicious activities and incidents of interest to the STAC as obtained from open and unclassified sources.